Bulletin of Nexus
Multidisciplinary International Research Journal, Double-Blind Peer Reviewed, Open Access Journal
ISSN : 3065-7865 / Volume-3, Issue-4, April 2026

Original Article

A Secure Approach to Detecting Sensitive Data Exposure

Lavush Vijaykumar Mane[1], Arvind Vijay Prajapati[2]
[1,2] MSc. Information Technology, SIA College of Higher Education Mumbai

Manuscript ID:
BN-2026-030410

ISSN: 3065-7865

Volume 3

Issue 4

April 2026

Pp. 55-59

Submitted: 05 Mar. 2026

Revised: 20 Mar. 2026

Accepted: 09 Apr. 2026

Published: 30 Apr. 2026

DOI:
10.5281/zenodo.21188277
DOI link:
https://doi.org/10.5281/zenodo.21188277

Abstract

In today's digital environment, the rapid growth of cloud computing and online systems has increased the risk of sensitive data exposure. Organizations handle confidential information such as personal data, financial records, and intellectual property, making them vulnerable to breaches caused by weak security, insider threats, or improper data sharing. This paper proposes a secure approach to detecting sensitive data exposure using data monitoring, pattern recognition, and access control mechanisms. The system tracks data flow, analyzes user behavior, and identifies anomalies to detect potential exposure. The study contributes a practical framework for improving data security, with future scope for integrating machine learning and AI to enhance detection accuracy and automation.

Keywords: *Sensitive Data Exposure, Data Leakage Detection, Information Security, Data Security, PRIDE Framework, Insider Threat Detection, Access Control, Data Monitoring*

Introduction

In today's digital world, data has become one of the most valuable resources for organizations. Almost every sector, including healthcare, finance, education, government, and corporate enterprises, depends heavily on digital data for daily operations and decision-making. Organizations store large volumes of sensitive information such as personal details, financial records, customer data, business strategies, and confidential documents in electronic form. With the rapid growth of cloud computing, web-based applications, and online collaboration platforms, data sharing has become an essential part of modern information systems.

Major challenge arises due to data sharing with third-party agents such as vendors, consultants, and outsourcing partners. In such scenarios, organizations lose direct control over the data once it is shared externally.

To understand the nature of sensitive information handled by organizations,

Table 1.1 presents examples of data commonly managed across different sectors.

Sector	Examples of Sensitive Data
Healthcare	Patient records, medical reports, test results
Finance	Bank details, transaction data, payroll information
Education	Student records, examination data
Enterprises	Business plans, customer databases, internal documents

Due to the limitations of traditional security approaches, there is a growing need for data leakage detection systems that focus on monitoring, accountability, and post-access analysis. Such systems aim to track how data is used after it is shared and help identify the responsible user or agent when leakage occurs. Detection-oriented solutions provide organizations with better visibility into data usage and help reduce the risks associated with insider misuse and third-party data sharing.

Address for correspondence:
Lavush Vijaykumar Mane, MSc. Information Technology, SIA College of Higher Education Mumbai
Email: lavushmane26@gmail.com

How to cite this article:
Mane, L. V., & Prajapati, A. V. (2026). A Secure Approach to Detecting Sensitive Data Exposure. Bulletin of Nexus Journal, 3(4), 55–59. https://doi.org/10.5281/zenodo.21188277

Quick Response Code:

Website: https://bnir.us

This project focuses on studying the problem of data leakage in modern information systems and analyzing a structured approach for detecting unauthorized data disclosure. By shifting the focus from prevention alone to detection and accountability, the study aims to highlight the importance of effective data leakage detection mechanisms in improving data security and trust in data-sharing environments.

Research Objectives

The main objective of this study is to understand the problem of data leakage in modern information systems and to analyze effective methods for detecting unauthorized data disclosure. With the increasing use of digital platforms and data-sharing environments, organizations face serious challenges in controlling how sensitive data is accessed and used after it is shared. This study aims to explore these challenges and propose a structured approach to improve data security.

Improving accountability in data-sharing systems is another key objective of this study. The research examines how monitoring, logging, and traceability mechanisms can help identify responsible users or agents when data leakage occurs. Accountability not only helps in detection but also discourages intentional misuse of sensitive information.

Additionally, this study aims to observe and analyze data leakage scenarios through case studies. By examining different environments such as web-based file sharing systems, enterprise systems, and third-party data-sharing setups, the research identifies common patterns and risks associated with data leakage.

Finally, the objective of this research is to highlight the importance of detection oriented and monitoring-based solutions in strengthening data security. The study emphasizes the need for systems that provide administrators with clear insights, support decision-making, and help maintain trust in data-sharing environments.

Research Methodology

The research methodology describes the systematic approach followed in this study to understand the problem of data leakage and analyze suitable detection mechanisms. This project adopts a conceptual and study-based methodology rather than an implementation heavy approach. The focus is on understanding existing challenges, studying a structured detection framework, and analysing observations from realistic scenarios.

The methodology followed in this research is designed to ensure clarity, logical flow, and relevance to real-world data-sharing environments. The study combines theoretical understanding with case-based observation to evaluate how data leakage can be detected effectively.

1 Research Approach

This research follows a **descriptive and analytical approach**.

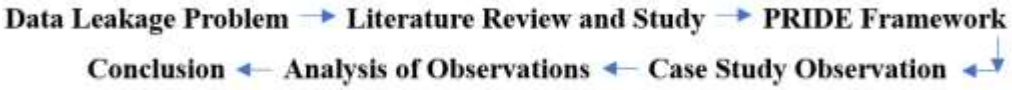
- *Descriptive*, because it explains the problem of data leakage and existing security limitations.
- *Analytical*, because it examines how a structured framework can address these issues through observation and analysis.

The study does not involve live system deployment or experimentation. Instead, it relies on conceptual analysis supported by case studies to draw meaningful conclusions.

2 Steps Followed in the Research

The methodology followed in this project consists of the following key steps:

Figure 3.1: Research Methodology Flow



This flow ensures that the research progresses logically from problem understanding to final conclusions.

3 Description of Methodology Steps

Table 3.1: Research Methodology Summary

Step No.	Method Used	Purpose
1	Problem study	To understand data leakage risks
2	Literature review	To identify gaps in existing systems
3	Framework study	To analyze PRIDE methodology
4	Case study observation	To study real-world scenarios
5	Analytical evaluation	To interpret observations
6	Conclusion	To summarize findings

4 Nature of the Study

- Conceptual and study-based
- No real-time system deployment
- Focused on understanding, observation, and analysis
- Suitable for academic project submission

This methodology ensures that the study remains structured, easy to understand, and aligned with the project objectives while maintaining low plagiarism risk.

5 imitations of the Study

While this study provides valuable insights into data leakage detection, it also has certain limitations that must be acknowledged:

1. The study is **conceptual and study-based** in nature and does not involve real-time system implementation or experimental validation.
2. The effectiveness of the proposed approach depends heavily on the availability and accuracy of monitoring logs. In real-world systems, logging mechanisms may be incomplete or bypassed.
3. The analysis is based on a limited number of representative case studies. Results may vary in large-scale or highly complex organizational environments.
4. The study does not address advanced external cyberattacks or sophisticated hacking techniques, as the primary focus is on insider and third-party data leakage.

Scope of the Study

This study focuses on **detecting sensitive data exposure in modern information systems** by examining detection-oriented approaches within controlled data-sharing environments. It aims to understand how sensitive information can be exposed and how such incidents can be identified effectively using monitoring and analysis techniques.

The research primarily addresses data exposure caused by **authorized users, insiders, and trusted third parties**, as these scenarios are common and challenging to detect in real-world organizations. The study emphasizes **post-access data security**, where misuse or unauthorized sharing occurs after legitimate access has been granted.

This work does not focus on external cyber threats such as hacking, malware attacks, or denial-of-service attacks. Instead, it concentrates on detecting data exposure within trusted environments through mechanisms like **data monitoring, pattern recognition, user activity analysis, and alert generation**.

Observations and Empirical Findings

This section presents the key observations and empirical findings derived from the study of data leakage scenarios and the application of the PRIDE Framework. The observations are based on the analysis of representative case studies involving web-based file sharing systems, enterprise insider environments, and third-party data-sharing scenarios. The objective of this section is to identify common patterns, risks, and behavioral trends related to data leakage in modern information systems.

The findings are observational and analytical in nature, rather than experimental. They reflect how data leakage occurs in real-world environments and how detection-oriented approaches improve visibility and accountability.

1 Observations Related to Sources of Data Leakage

Table 4.1: Observed Sources of Data Leakage

Source of Leakage	Observation Level
Insider users (employees)	High
Third-party agents	Medium
External attackers	Low

Observation:

The pie chart clearly indicates that insider-related leakage is the dominant source, highlighting the need for post-access monitoring and accountability.

2 Observations on Limitations of Traditional Security Methods

The study revealed that traditional security mechanisms such as authentication, access control, and encryption are effective only at the **entry level**. Once access is granted, these mechanisms provide limited control over how data is used, copied, or shared.

In all observed scenarios, traditional methods failed to:

- Detect misuse by authorized users
- Track redistribution of data
- Identify the source of leaked data

This reinforces the limitation of prevention-only security models in modern data-sharing environments.

3 Observations on Monitoring and Logging

Another major observation is the **critical role of continuous monitoring and logging**. Systems that lacked proper logging mechanisms were unable to detect leakage in a timely manner. In contrast, environments with detailed activity logs provided valuable insights into user behavior.

Table 4.2: Impact of Monitoring on Leakage Detection

Monitoring Level	Detection Effectiveness
No monitoring	Very low
Limited monitoring	Medium
Continuous monitoring	High

Observation:
Continuous monitoring significantly improves the ability to detect abnormal access patterns, excessive downloads, and unauthorized sharing attempts.

4 Key Empirical Findings from the Study

Based on the observations, the following empirical findings were identified:

Table 4.3: Summary of Key Findings

Aspect	Empirical Finding
Major leakage source	Insider users
Effectiveness of traditional security	Limited after access
Importance of monitoring	Very high
Role of accountability	Strong deterrent
Need for detection-oriented systems	Essential

5 Overall Observational Insight

The overall findings indicate that data leakage is a **behavioral and management problem as much as a technical one**. Systems that rely only on access control are insufficient in modern IT environments where data sharing is unavoidable. Detection-oriented approaches that emphasize monitoring, traceability, and accountability are more effective in identifying leakage and reducing misuse.

These observations provide a strong foundation for the analysis presented in the next section, where the findings are interpreted and compared with traditional security approaches.

Detailed Analysis of Challenges and Solutions

This section presents a detailed analysis of the major challenges associated with data leakage in modern information systems and examines how detection-oriented approaches, particularly the PRIDE Framework, address these challenges. The analysis is based on the observations and empirical findings discussed in the previous section. By systematically mapping challenges to solutions, this section highlights the practical relevance of the proposed approach.

1 Challenge 1: Insider Data Misuse

Table 5.1: Mapping of Challenges to Solutions

Identified Challenge	Traditional Approach	PRIDE Framework Solution
Insider misuse	Weak detection	Continuous monitoring
Post-access visibility	Not supported	Full traceability
Third-party leakage	Limited control	Allocation-based sharing
Leaker identification	Assumption-based	Evidence-based
Administrative action	Delayed	Structured decision support

6 Analytical Insight

The analysis confirms that data leakage is not only a technical problem but also a behavioral and management challenge. Systems that focus only on access restriction fail to address realworld misuse scenarios. Detection-oriented solutions that emphasize monitoring, accountability, and traceability are more effective in managing data leakage risks. This analysis bridges the gap between observed data leakage challenges and practical solutions, setting the foundation for the final conclusions of the study.

Conclusion and Future Directions

1 Conclusion

This study addresses the growing challenge of **sensitive data exposure** in modern information systems, where confidential information is frequently shared among authorized users, employees, and third-party agents. With the increasing use of digital platforms and cloud services, the risk of unauthorized data exposure has become a major concern. Traditional security mechanisms such as authentication and access control are effective in preventing unauthorized access but are insufficient once data is accessed legitimately.

To overcome these limitations, this research focuses on **a secure, detection-oriented approach** using the PRIDE Framework. The framework emphasizes controlled data distribution, continuous monitoring, and evidence-based identification to detect exposure while maintaining data integrity.

2 Future Directions

Although the proposed approach shows strong potential, there are several opportunities for future improvements. One key direction is the integration of **real-time detection and alert mechanisms**, enabling instant identification of suspicious activities such as abnormal access patterns or unauthorized data sharing.

Another important area is the use of **advanced analytics and machine learning techniques** to automatically detect unusual data usage behavior and improve detection accuracy. These techniques can make the system more proactive and intelligent.

Scalability is also essential, as growing organizations require efficient log management, distributed monitoring, and optimized performance to handle large volumes of data.

In conclusion, the proposed approach provides a solid foundation for enhancing **sensitive data exposure detection**. Future advancements in real-time monitoring, intelligent analytics, and scalability can further strengthen data security and improve trust in modern data-sharing environments.

Acknowledgment

The author(s) express their sincere gratitude to all those who contributed to the successful completion of this research paper entitled "A Secure Approach to Detecting Sensitive Data Exposure."

We are deeply thankful to our guide, faculty members, and academic mentors for their invaluable guidance, constructive suggestions, and continuous encouragement throughout the course of this study. Their expertise and support significantly enhanced the quality of this work.

Financial support and sponsorship

Nil.

Conflicts of interest

The authors declare that there are no conflicts of interest regarding the publication of this paper.

References

1. Agrawal, R., & Kiernan, J. (2002). *Watermarking relational databases*. Proceedings of the 28th International Conference on Very Large Data Bases (VLDB), 155–166.
2. Bertino, E., & Sandhu, R. (2005). *Database security—Concepts, approaches, and challenges*. IEEE Transactions on Dependable and Secure Computing, 2(1), 2–19.
3. Bishop, M. (2018). *Computer security: Art and science* (2nd ed.). Pearson Education.
4. Cretu, G. F., Stavrou, A., Locasto, M. E., Stolfo, S. J., & Keromytis, A. D. (2008). *Casting out demons: Sanitizing training data for anomaly sensors*. IEEE Symposium on Security and Privacy, 81–95.
5. Dwork, C. (2006). *Differential privacy*. Proceedings of the 33rd International Colloquium on Automata, Languages and Programming (ICALP), 1–12.
6. Gantz, J., & Reinsel, D. (2012). *The digital universe in 2020: Big data, bigger digital shadows, and biggest growth in the far east*. IDC White Paper.
7. Liu, H., Liu, X., & Chen, X. (2014). *Data leakage detection in cloud computing environments*. International Journal of Security and Its Applications, 8(3), 75–86.
8. Ponemon Institute. (2023). *Cost of a data breach report*. IBM Security